中华人民共和国国家标准

计算机软件可靠性和可维护性管理

Software reliability and maintainability management

GB/T 14394—93

1 主题内容与适用范围

本标准规定了软件产品在其生存周期内如何选择适当的软件可靠性和可维护性管理要素，并指导软件可靠性和可维护性大纲的制定和实施。

本标准适用于软件产品生存周期的各个阶段。

2 引用标准

GB 6992 可靠性与维修性管理

GB 8566 计算机软件开发规范

GB/T 11457 软件工程术语

3 术语和定义

本标准将采用 GB/T 11457 中术语和定义。此外强调给出下列术语和定义。

3.1 软件可靠性 sofrware reliability

a. 在规定环境下，在规定时间内软件不引起系统失效的概率。

b. 在规定的时间周期内所述条件下程序执行所要求的功能的能力。

3.2 软件可维护性 software maintainability

与进行规定的修改难易程度有关的一组属性。

3.3 软件生存周期 software life cycle

软件产品从形成概念开始，经过开发、使用和维护，直到最后不再使用的整个过程。

3.4 软件可靠性和可维护性大纲（以下简称大纲） software reliability and maintainability program

为保证软件满足规定的可靠性和可维护性要求而制订的一套管理文件。

4 软件生存周期

4.1 软件生存周期各阶段对可靠性和可维护性要求

本标准按 GB 8566 划分软件生存周期。强调各个阶段软件可靠性和可维护性要求。

4.1.1 可行性研究与计划阶段——进行项目可行性分析。制订初步项目开发计划，提出软件可靠性和可维护性目标、要求及经费，并列入合同（或研制任务书，下同）。

4.1.2 需求分析阶段——将合同的技术内容细化为具体产品需求。分析和确定软件可靠性和可维护性的目标，制定大钢及其实施计划。

4.1.3 概要设计阶段——进行可靠性和可维护性目标分配，进行可靠性和可维护性概要设计，并明确对详细设计的具体要求。

4.1.4 详细设计阶段——进行软件可靠性和可维护性详细设计，编写相应的设计说明，明确对实现阶段的具体要求。

国家技术监督局 1993-05-01 批准　　1994-01-01 实施

4.1.5 实现阶段——进行单元测试,分析和验证有关软件可靠性和可维护性的部分要求。
4.1.6 组装测试阶段——进行组装测试,并进一步分析软件可靠性和可维护性。
4.1.7 确认测试阶段——确认软件产品的可靠性和可维护性是否达到预定的目标。
4.1.8 使用和维护阶段——采集数据,定期评价,加强维护管理,以确保软件的可靠性和可维护性增长。

4.2 软件生存周期可靠性和可维护性度量方法

在软件生存周期的各个阶段,应进行与可靠性和可维护性有关的度量,度量方法通常分定性的估计、定量的预测和测量等等。具体方法的选择应视软件所处的阶段和其活动而定,其目的是保证在软件生存周期的特定阶段的关键问题能得到及时解决。

5 软件可靠性和可维护性大纲

根据合同或协议书中对软件可靠性和可维护性的要求编制大纲,大纲的制定和修改应按质量保证有关标准规定的程序进行评审和审批,大纲的实施应由主管机构和软件开发项目各层次负责人分工负责。同时纳入软件开发计划,并与系统管理相结合,充分考虑技术及成本因素实施综合管理。

5.1 制定大纲应考虑的主要因素:

编制大纲,应考虑如下因素:

a. 所处生存周期阶段;

b. 规定的可靠性和可维护性目标;

c. 每项活动的主要任务;

d. 拟采用的开发技术和类似软件的历史状况;

e. 时间进度、经费与其他资源,存储空间与运行时间,程序设计语言,软件运行的软、硬件环境等各种限制条件。

5.2 大纲应包括的主要活动项目

以下条款给出了软件可靠性和可维护性大纲要素,并对这些要素的应用及任务进行了描述。

5.2.1 制定大纲计划和目标

在需求分析阶段,应该建立软件产品的可靠性和可维护性大纲计划。大纲计划由一系列的与每项大纲要素有关的任务组成,应明确每项任务的责任,并提供一个任务实施初步日程表,当情况变化或出现偏差时计划应根据需要加以修改。

大纲计划应定量和定性地建立目标,并说明验证所需的判据和条件。

a. 大纲制定和实施所需的组织机构和职责;

b. 定量、定性的可靠性和可维护性目标(如:可靠度 R(T)、失效发生率 ROCOF,等等);

c. 各项任务实施进度表;

d. 可靠性和可维护性估计及验证所用的判据;

e. 软件版本控制及标准化要求;

f. 评审计划;

g. 文件编制要求;

h. 培训及支持保证计划;

i. 测试计划。

5.2.2 分析运行环境

在可行性研究与计划及需求分析阶段应分析运行环境,并在概要设计和详细设计阶段进行必要的修改,同时要注意运行环境的变化会对软件的可靠性和可维护性的影响。

下列运行环境和最终使用条件应该分析:

a. 运行的系统及体系结构;

b. 运行和维护方式；

c. 负载；

d. 运行和维护环境（如电磁辐射和感应）；

e. 运输和安装条件；

f. 操作和维护人员要求；

g. 新版本的发行和升级；

h. 恢复的规程和要求；

i. 终端和通信媒体类型。

5.2.3 软件可靠性和可维护性要求的可行性论证

在可行性研究与计划阶段，应对软件的可靠性和可维护性要求进行可行性论证，对于合同中提出的软件可靠性和可维护性要求应根据软件符合规定标准和规范的能力进行评审和论证。这个论证是整个产品研究的一部分，其目的是：

a. 确定设计工作的起点。

b. 估计可靠性和可维护性特性对技术选择，设计配置以及产品性能满足市场需求能力的影响。

c. 估计弥补现有产品与新一代产品原理上的差距所带来的成本影响和承担的风险。

应该考虑：

a. 软件的功能需求；

b. 新软件的市场潜力；

c. 现有软件的技术状况；

d. 生存周期费用；

e. 开发新软件与改造现有软件所付出的劳动的比较。

5.2.4 选定或制定规范和准则

在需求分析阶段，应选定适当的软件规范和准则。若没有适当的软件规范和准则可遵循，则应自行制定。其内容包括：

a. 确保软件可靠性和可维护性所必须的软件工程规范；

b. 制定软件开发必须遵循的技术准则；

c. 制定软件的支持和维护要求；

d. 必要时制定外购、转承开发和重用原有软件的可靠性和可维护性控制规范。

5.2.5 软件可靠性和可维护性分析

在软件开发过程中各个阶段进行有关的软件可靠性和可维护性分析并编写分析报告应考虑：

a. 可靠性和可维护性目标分配；

b. 软件使用需求量过载情况；

c. 程序设计中的实施情况；

d. 可靠性和可维护性预测；

e. 故障模式、影响及危害度分析；

f. 根源分析；

g. 关键模块分析；

h. 故障定位和隔离技术的应用；

i. 测试环境、测试系统、测试用例和测试覆盖情况；

j. 维护实施简易性。

5.2.6 评审

在软件开发各阶段都要求进行评审，评审管理要求按 GB 8566 进行，其中与软件可靠性和可维护性有关的具体评审要求如下：

5.2.6.1 需求分析评审

a. 可靠性和可维护性目标；

b. 大纲及其实施计划；

c. 操作顺序和不可逆操作顺序的保障要求；

d. 功能降级使用方式下，软件产品最低功能保证的规格说明。

e. 选用或制定的规范和准则。

5.2.6.2 概要设计评审

a. 可靠性和可维护性目标分配；

b. 可靠性和可维护性设计方案；

c. 设计分析，关键成分的时序，估计的运行时间，错误恢复及相关性能要求；

d. 测试原理、要求、文件和工具。

5.2.6.3 详细设计评审

a. 各单元可靠性和可维护性目标；

b. 可靠性和可维护性设计(如：容错)；

c. 测试文件；

d. 软件开发工具。

5.2.6.4 软件验证与确认计划评审

a. 软件可靠性和可维护性验证和确认方法；

b. 软件可靠性和可维护性测试(计划、规程、用例和设施)；

c. 验证与确认时所用的其他准则。

5.2.7 文件和数据

根据合同要求和数据管理目标，确定文件和数据要求的范围。

大纲应建立一个报告事件及其结果的系统。该系统应提供数据可追溯性，并建立相应文件，文件应写明具体数据的采集条件、所作的设想，并注明对数据应用的限制。为保证关键事件得到明确认识，该系统应提供充分的数据，并且系统的输出应适合接受者的需要和分发的要求。

应监视以下关键事项：

a. 大纲目标的建立；

b. 可靠性和可维护性目标分配；

c. 模块一览表的制定；

d. 测试；

e. 故障发生；

f. 缺陷和错误的检查；

g. 维护活动；

h. 恢复活动；

i. 数据分析；

j. 采取的纠正措施和结果。

5.2.8 培训

要求及时制定培训计划。培训计划应与软件开发计划、维护要求、运行支持策略协调一致。培训对象包括软件开发人员、维护人员、质量控制人员、管理人员、操作人员，针对不同对象进行不同类型、不同级别的培训。培训内容为：

a. 一般知识或专门技术；

b. 软件的复杂性；

c. 操作要求；

d. 需用的时间和资源；

e. 需用的设施和工具。

5.2.9 维护保障要求

对维护保障要求应进行说明并制定计划。需考虑下列因素：

a. 维护和后勤保障策略；

b. 技术保障功能；

c. 维护保障任务；

d. 配置管理；

e. 操作和修改规程；

f. 突发事件和分析；

g. 数据采集和现场跟踪；

h. 文件。

5.3 示例

表1说明了大纲的各项活动同软件生存周期各阶段的基本关系，它为适当地选择相关大纲任务提供一个示例。

5.4 剪裁

大纲内容可根据软件类别、规模和关键程度作适当剪裁。剪裁原则是：所制定大纲能使软件开发以最佳费用效益实现规定的可靠性和可维护性要求。

表 1 软件生存周期阶段与可靠性和可维护性大纲要素对应关系

生存周期阶段	5.2.1 制定大纲计划和目标	5.2.2 分析运行环境	5.2.3 软件可靠性和可维护性要求的可行性论证	5.2.4 选定或制定规范和准则	5.2.5 软件可靠性和可维护性分析	5.2.6 评审	5.2.7 文件和数据	5.2.8 培训	5.2.9 维护保障要求
可行性研究与计划		√	√		√		√		
需求分析	√	√		√	√	√	√		√
概要设计					√	√	√	√	√
详细设计					√	√	√		√
实现					√		√	√	√
组装测试					√	√	√	√	√
确认测试					√	√	√	√	√
使用和维护					√		√	√	√

注："√"表示该阶段所需考虑的有关任务条款。

附加说明：

本标准由中国标准化与信息分类编码研究所提出并负责起草。

本标准主要起草人戚奎桐、何国伟、王纬、陈崇昕、徐树森。